EDC 2021/573326 CONTRATE UN CIBERSEGURO

F. de publicación 7 de junio de 2021

Un *hacker* informático ha bloqueado todo el sistema de una empresa que, en consecuencia, no puede operar ni recibir cobros, lo que le está acarreando graves perjuicios. Recuerde que hay seguros que cubren estas contingencias...

Ciberataques

Datos. No es necesario ser una gran empresa para sufrir un ciberataque. De hecho, la mayoría de víctimas son PYMES, y los delincuentes buscan acceder a sus bases de datos para bloquearlas y pedir un rescate. **¡Atención!** Vea los riesgos que asumiría su empresa ante un ciberataque:

- Los *hackers* pueden bloquear la operativa de la empresa, que no podrá servir pedidos ni pagar facturas y nóminas. **¡Atención!** Aunque haya sufrido un ataque, su empresa sigue siendo responsable de sus obligaciones.
- Asimismo, los *hackers* tienen acceso a los datos de clientes y proveedores, lo que pueden aprovechar, por ejemplo, para solicitar que efectúen los pagos a sus cuentas.
- Además, al quedar expuestos los datos personales de sus clientes, estaría incumpliendo, aunque involuntariamente, la Ley de Protección de datos (LPD), con riesgo de sanciones.

Brecha. Un ciberataque que exponga los datos personales que maneja su empresa supone una "brecha de seguridad", brecha que deberá notificar a la Agencia de Protección de Datos y a los afectados cuyos datos hayan quedado expuestos. **¡Atención!** Ello no implica necesariamente una sanción, pero sí que se iniciará un procedimiento donde se verificará que su empresa dispone de las medidas de seguridad adecuadas para proteger los datos personales que maneja.

Ciberseguro

Garantías. En todo caso, sepa que existen seguros que cubren los riesgos derivados de un ciberataque. A la hora de escoger la póliza, asegúrese de que cubre, además de la defensa jurídica, los siguientes riesgos (como mínimo):

- *Frente a terceros.* Las cantidades que la empresa esté obligada a pagar por cualquier reclamación de incumplimiento involuntario de la normativa de protección de datos.
- *Frente a organismos reguladores.* Las sanciones impuestas por dicho incumplimiento.
- *Por publicaciones en Internet.* Las reclamaciones de los perjudicados cuando el ataque consista en difundir falsedades en la red sobre un tercero.
- *Sanciones y pagos relacionados con tarjetas de pago de terceros* . Cuando, por ejemplo, fruto del fallo de seguridad sea saqueada la tarjeta de pago de un tercero.
- *Interrupción del negocio.* Indemnización por pérdida de beneficios y gastos fijos permanentes a consecuencia de un incidente cubierto por la póliza.

Análisis previo. Tenga en cuenta que al contratar la póliza la compañía hará un análisis de las medidas de seguridad existentes en su empresa (o de las que necesita). La existencia de estas medidas más la existencia del propio seguro le dará máxima garantía para reducir riesgos.

Daños propios

Actuaciones. Asegúrese de que el producto que contrata contemple actuaciones inmediatas y de contingencia, con servicio de asistencia 24 horas, gestión de incidentes para recuperar la normalidad lo antes posible, comunicación a la Agencia de Protección de Datos de la brecha de seguridad, y recuperación y reposición de los datos perdidos. **Apunte.** Si tiene un seguro, será muy difícil que le sancionen en caso de ciberataque.

A la hora de contratar el seguro la compañía analizará si sus medidas de seguridad son adecuadas. El mantenimiento de unas medidas adecuadas y la cobertura del propio seguro reducirán el riesgo de daños ante un ciberataque.